Transmit Filter and Multi Secrecy Aided Optimization with DFE for Duplex Systems

Shilpa Mariam Saji[1], *Mithra ST*[2]
[1]*M.tech(Scholar), Communication Engineering, Department of ECE, Sree Buddha College of Engineering, Ayathil, Kerala, India*
[2]*Assistant Professor, Department of ECE, Sree Buddha College of Engineering, Ayathil, Kerala, India*

***Abstract*—This paper focuses on the problem of secure transmission in wireless communication, especially in the physical layer. In Cyber-Physical systems, interconnected devices under wireless environments facilitate information exchange but challenge network security. In order to proliferate secrecy, with the assumption of channel reciprocity, the legitimate users share the same channel which is independent of the channels between the legitimate users and the eavesdropper. It is because of the broadcast nature of the wireless medium makes it vulnerable to two types of major attacks denial of service, and information leakage. Here the security may decrease due to the correlation between the generated secret bits. To address these challenges, this framework includes two multi-antenna legitimate parties and a multi-antenna eavesdropper node. In order to maximize the secrecy rate, interleaver along with jointly optimized transmit filter and multi secrecy techniques are used at transmitting section. Optimum receive filter and Equalization technique are used at the receiver section. At last, this paper provides channel estimation errors and self-interference implemented for both duplex systems. So combining with them is a kind of key technology in future physical layer wireless communication.**

***Keywords*—MIMO-OFDM, jamming, DFE, CPS, Artificial noise, Physical layer security, Interleaver**

I. INTRODUCTION

Wireless technologies are emerging very fast, as the latest technologies allow users to access information and services via electronic media. As wireless networks are becoming more sophisticated and offering more applications, the confidentiality of data need to be preserved. Due to the mobility of devices, channel instability, broadcast nature of networks and dynamic topology, they are vulnerable to various security issues and threats like DoS, tampering, leakage, and interference. Attackers with a transceiver can be able to hinder wireless transmission. Thus there is a need to cope up with various security issues. In this paper, the secrecy rate is attained by the joint optimization of transmit filter and multi secrecy techniques. This optimization will improve secrecy better than existing methods in military applications, business field, online banking, and ATM services.

This paper is divided into six sections, the first is the introduction. Section II introduces the existing system. A new technology MIMO-OFDM system is presented in section III. Proposed duplex systems are evaluated in section IV. Simulation results and conclusions are given in sections V and VI, respectively

II. LITERATURE SURVEY

The security techniques in the physical layer of the communication system aim to harden the secrecy characteristics, thereby decreasing the signal quality of a prospective eavesdropper. Secret transmit beamforming approach using optimization of the transmit weights and Artificial noise (AN) in Half Duplex (HD) system is presented in [2] with the Channel state information of the intended receiver and eavesdroppers. Total power optimized is 18.05 dB. Full duplex (FD) system with beamforming and power optimization techniques are discussed in [3] by using maximum ratio combining (MRC) and optimal combining (OC) schemes in the presence of self-interference due to FD transmission. Power optimized is 19.59 dB. In multiuser broadcast channel, the eavesdropper is interested in any particular stream transmitted by the BS.

A normalized linear precoding matrix (LP) and cooperative jamming (CJ) is illustrated in [4] could interfere Eve to help the BS to communicate confidentially with the legitimate users to enhance the physical layer security. A multi-cell full-duplex MIMO scenario is presented in [5].Transmit and receive filters are designed with a weighted sum rate (WSR) maximization problem, using both individual and sum power constraints. A joint transmit filter and AN optimization framework is introduced in [1] for the wireless duplex communication systems.Zero Forcing (ZF) and optimum filter are compared at the receiver filter and evaluate their performance. Power optimized is 14.23dB

However, with the eavesdroppers overhearing capacity goes increases and as mobility of devices increases, this artificial noise based security technique is not enough secure.

III. MIMO - OFDM SYSTEM

An antenna technology called Multiple-input multiple-output (MIMO), incorporate with orthogonal frequency division multiplexing (MIMO-OFDM) is an advanced air-interface solution for next-generation wireless systems[6,7]. As the MIMO technology increases capacity, thereby multiple signals send over multiple antennas. The orthogonal frequency-division multiplexing (OFDM), which divides a radio channel into a large number of closely spaced sub-channels to provide more reliable communications at high speeds and spectral efficiency. MIMO incorporated OFDM system is a promising technique for higher capacity for multi-hop networks.

A. MIMO System

The MIMO system moreover multiplies the radio link capacity thereby transmitting multiple information bearing signals over multiple, co-located antennas. It is accomplished without the need for additional power or bandwidth. In a MIMO system, the user data is broken down into several chunks and transmitted over the antennas by using the same frequency Fc. For a given subcarrier, QPSK symbols are transmitted on several antennas (MIMO). And an antenna can transmit several subcarriers (OFDM).

B. Orthogonal Frequency Division Multiplexing

In general, Orthogonal Frequency Division Multiplexing (OFDM) is a multicarrier modulation technique in which FDM modulation technique for transferring huge amount of data over a radio wave preserving bandwidth efficiency. As its name implies it is orthogonal FDM i.e carrier centers are put on orthogonal frequencies. The peak of each signal coincides with zero crossings of other signals. While the symbol transmitting through the channel, past symbols interfere with present symbols create ISI. Equalization is a technique to avoid ISI. Another technique to remove ISI more efficiently is OFDM.

IV. SYSTEM MODEL

There is often transmission modes are used for delivery of data between communication devices. In communication networks, there are commonly two modes of communication. ie, simplex and duplex. Here OFDM technique is applied to both duplex systems[1].

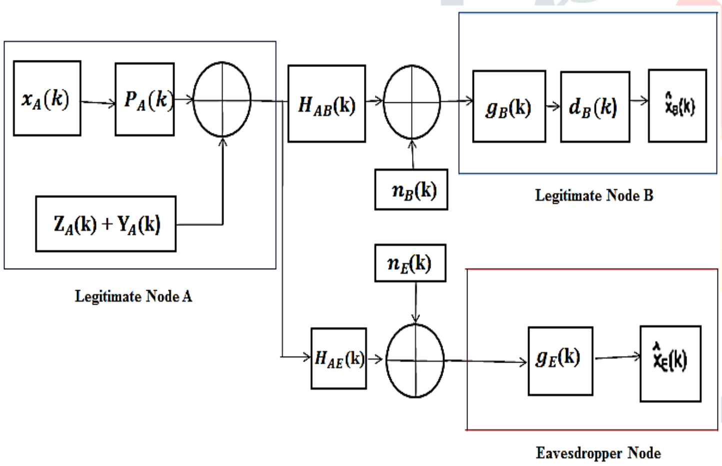

Fig.1: Half duplex system model

A. Half Duplex System Model

The half-duplex system model is given in Fig.1. The complete block diagram of OFDM induced multi secrecy technique is illustrated here. Packet transmission is carried out at the physical layer.

The binary bits to analog signal transformation are conducted and the waveform is sent over a communication channel.

A. Transmission Section

The transmission section illustrated in Fig.2 contains interleaver, channel encoder, modulator, transmit filter cum artificial and phase noise, IFFT, and cyclic prefix.

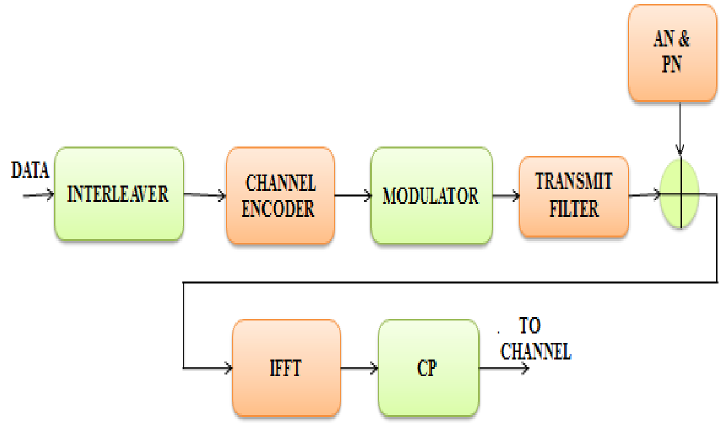

Fig.2: Transmission section

B. Interleave

The basic idea behind the use of interleaved codes is to scatter input symbol sequence at transmitter. It leads to alter sequence at receiver also. However, deinterleaver will alter the received sequence to get back the original unaltered sequence at transmitter.

C. Channel Encoder

The information bits are encoded by convolution encoder, converts serial data into parallel data[8,9]. Check bits are interleaved with data. Thus it helps to correct an error in whole blocks.

D. Modulator

Data is now modulated by a 16-QAM modulator mapping onto the sub-carrier amplitude and phase. In communications systems, Quadrature Amplitude Modulation (QAM) is implemented utilizing both amplitude and phase variations.

E. Multi Secrecy Techniques

Multi secrecy techniques merely contain two techniques which intensify existing secure communication. In this approach there includes artificial noise [1,10,11] and phase noise signals for improving physical layer secrecy. Thus the confidentiality of the data transmission can be improved. The power invested in each of them is calculated.

F. Phase Noise

With the newly emerging concept of phase jamming, the phase of the information signal is changed, with the complete knowledge of legitimate receiver for information security. The main idea is to change the phase of the transmitted signal, which prevents the unauthorized user to receive the signal in correct phase. These noise components are known by legitimate receiver. The power invested in multi-secrecy technique is treated as

$$P_{AN+PN} = \sum_{k=0}^{K} \mathrm{Tr}\big(\phi(k) + \alpha(k)\big) \ldots\ldots\ldots\ldots\ldots (1)$$

where, $\phi(k) + \alpha(k)$is the covariance matrix of corresponding noises$z_A(k)$ and$y_A(k)$

G. Transmit Filter

The transmit filter at the transmission section reduces the noise generated by the base station. Thus it provides pulse shaping and optimizes power consumption. It also eliminates the wideband noise created by the transmission system.

H. IFFT

Inverse Fast Fourier Transform (IFFT) and Fast Fourier Transform(FFT) operation ensure that subcarriers do not interfere with each other. i.e. OFDM is spectrally efficient.It perform operation (I+jQ)exp(jωct). Input bits are mapped on the I and Q components of the QAM symbols and arranging in a proper length as the number of subcarriers in the OFDM symbol.To transmit data, the signal must be represented in the time domain.

I. Cyclic Prefix

In order to avoid inter-carrier interference (ICI), each of the OFDM symbols is preceded by a copy of the end part of that same symbol. It provides a guard interval between OFDM symbols. Thus preserves the orthogonality between subcarriers.

J. Receiver Section

As there are multiple antennas at the receiver section, high data rate and reliability are preserved. The binary data obtained is an estimate of the transmitted binary information. Received signals at corresponding nodes are expressed as

$$r_B(k) = H_{AB}^{H}(k)\,(s_A(k) + (z_A(k) + y_A(k)) + n_B(k)$$
$$r_E(k) = H_{AE}^{H}(k)\,(s_A(k) + (z_A(k) + y_A(k)) + n_B(k) \qquad ....(2)$$

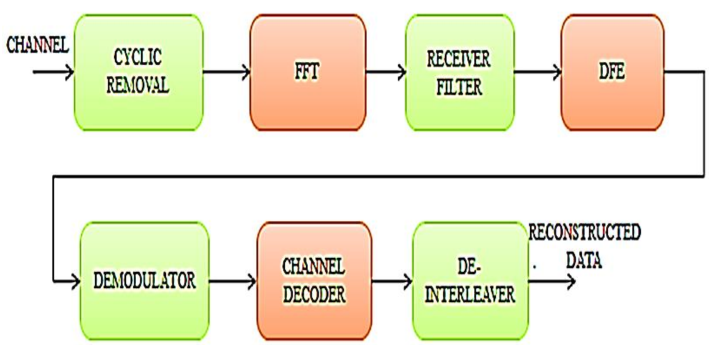

Fig.3: Receiver section

Consider the ZF filter and an Optimum filter and comparison is performed to obtain a better solution. The name Zero Forcing corresponds to bringing down the interference of data to zero at the received signal. The optimal linear receive filter is obtained for acquiring the best estimate of the desired signal from a noisy measurement. It is done by minimizing the MSE. The SNIR of corresponding nodes is obtained.

As it is known that use of a cyclic prefix is standard within OFDM and it enables the performance to be maintained even under conditions when levels of reflections and multipath propagation are severe.However, FFT converts the time domain samples back into the frequency domain. Actually, demodulator is an electronic circuit in which the information content is recovered from the modulated carrier wave. The QAM demodulator is the reverse of the QAM modulator. Finally, the parallel to serial block converts this parallel data into a serial stream to recover the original input data is decoded by viterbi algorithm.

K. Decision Feedback Equalizer

Intersymbol interference (ISI) is actually an unwanted phenomenon of the form of a distorted signal in which one symbol interferes with subsequent symbols. Distortion on a current pulse as it was caused by previous pulses is subtracted. The decision feedback equalizer(DFE) will estimate the current symbol from previous symbols by predicting the noise level of the channel through noise predictor. Then predicted noise is subtracted from the input signal by using a feedback filter(FB) to reduce the noise level of the channel [12,13,14]. In other words, DFE is actually a filter that uses the feedback of detected symbols to produce an estimate of the channel output. Estimated signal

$$\hat{x}_A^B(k) = g_B(k)\, d_B(k)\, r_B(k) \qquad ....(3)$$

where, $d_B(k)$ is the DFE

B. Full Duplex System Model

The legitimate nodes A and B send information signal along with multi secrecy components. As it is a full duplex system, the eavesdropper node gets affected by the interference due to simultaneous transmission along with the artificial noise and phase noise components[15]. A full duplex system model is illustrated in Fig.4.All analysis in full duplex is similar to half duplex, except there is dual communication occurs at the same time.

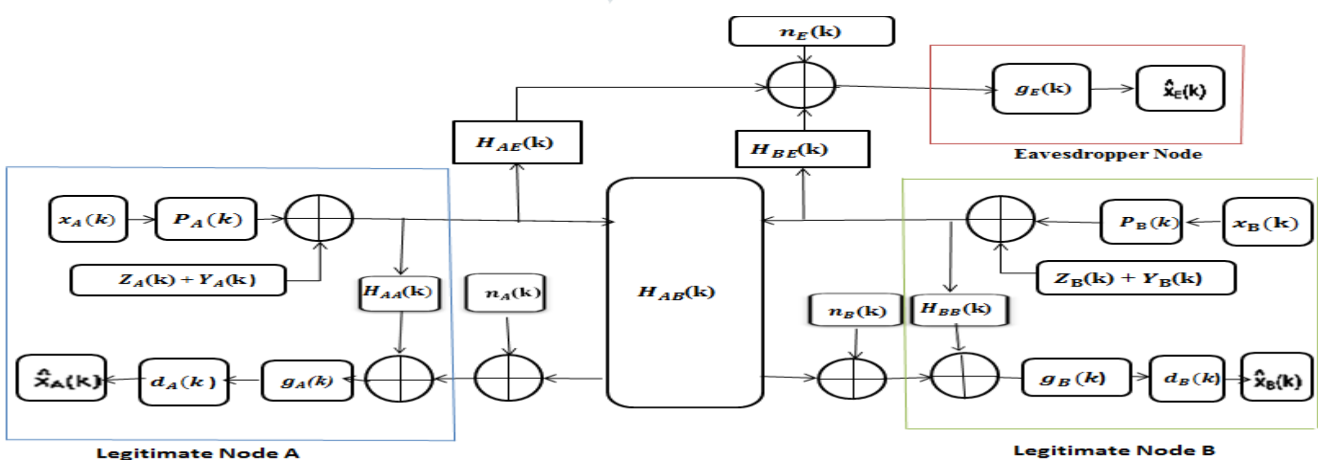

Fig.4: Half duplex system model

V. SIMULATION RESULT

In this section performance of duplex systems are treated by MATLAB programming.

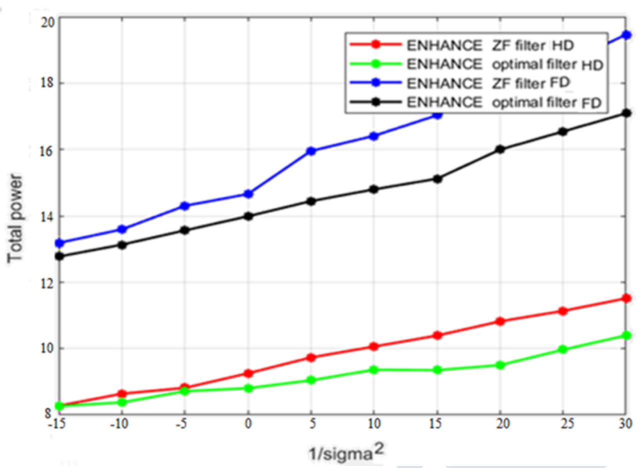

Fig.5: Power consumption in duplex systems

Power consumption of the duplex system is illustrated in fig.5. As large 1/sigma^2 means strong overhearing ability of eavesdropper, while smaller the value means weak overhearing ability. FD system performs better than HD.

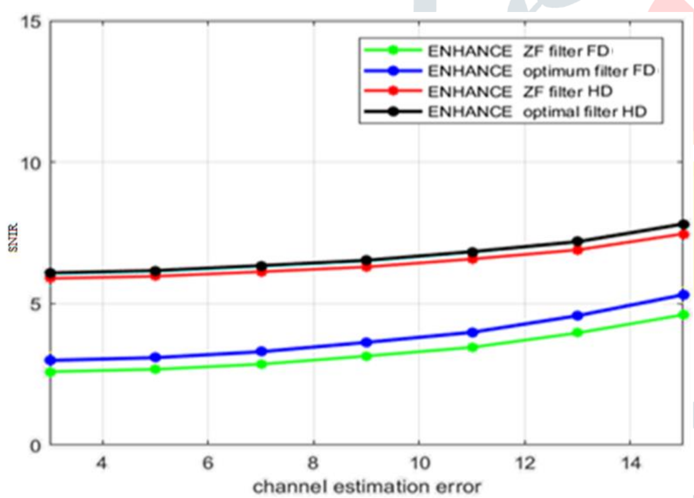

Fig.6: SNIR vs channel estimation error

Channel estimation error factor is in fig.6. It is evident that FD systems cause interference than HD systems due to simultaneous transmission. So as interference increase, SNIR value reduces in FD systems and in HD systems vice-versa.

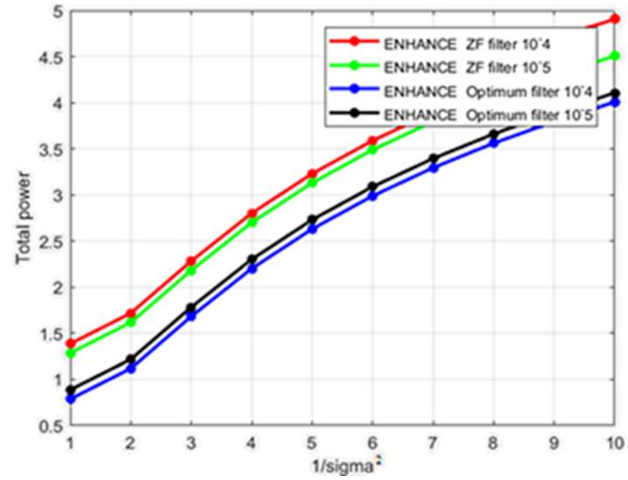

Fig.7: Self-interference coefficient in duplex systems.

The impact of self- interference coefficient is shown in Fig.7.As the residual self- interference coefficient increases[1], the total power of the system also got an increase. So to reduce power consumption, inference value got reduced. In FD systems, efficient self-interference cancelation schemes are to be properly working, to minimize interference problems.

VI.CONCLUSION

Over the years, there has been tremendous growth in digital communications especially in the fields of multimedia, teleprocessing, graphic design, cellular, satellite, and computer communication. Hence, information security has become a key challenge, attain confidentiality in existing communication techniques, physical layer security is an alternative paradigm to protect the wireless transmission against eve's attacks.FD with AN and PN system has better performance than the other systems when there is successful SIC. Here a joint transmit filter and multi-security optimization scheme is devised, to minimize error rate and attain a target secrecy level. This joint optimization framework is well suited for making physical layer security in wireless transmission systems.

REFERENCES

[1] O. Cepheli, G. Dartmannz, G.K.Kurt, and G.Ascheid, "*A Joint Optimization Scheme for Artificial Noise and Transmit Filter for Half and Full Duplex Wireless Cyber Physical Systems*"IEEETransactions on Sustainable Computing, 2017

[2] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," IEEE Transactions on Signal Processing,,vol. 59, no. 3, pp. 1202 –1216, March 2011.

[3] O. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," IEEE Communications Letters, vol. 18, no. 6, pp. 1075–1078, June 2014.

[4] J. Yang, I. M. Kim, and D. I. Kim, "Joint design of optimal cooperative jamming and power allocation for linear precoding," IEEE Transactions on Communications, vol.62, no.9, pp. 3285–3298, Sept 2014.

[5] A. C. Cirik, O. Taghizadeh, L. Lampe, R. Mathar, and Y. Hua, "Linear transceiver design for full-duplex multi-cell MIMO Systems," IEEE Access, vol. 4, pp. 4678–4689, 2016.

[6] Wang Junxuan "Effect of Channel Estimation Error on MIMO-OFDMSystems Capacity"6th International Conference on Wireless Communications Networking and Mobile Computing,October 2010

[7] H. Bölcskei, and E. Zurich "*MIMO - OFDM wireless systems: basics, perspectives, and challenges.*" IEEE Wireless Communications,August 2006.

[8] J. Kaur, S. Kaur and Sandhu"*Comparison of BER for various Constraint Lengths of Convolution Coding in OFDM System*"IJARECE Volume 5, Issue 5, May 2016

[9] https://wiki.cse.buffalo.edu/cse545/content/burst-error-correcting-codes CSE 545: Coding Theory

[10] M.I.Khan and M.Riaz “Comparison of different types of physical layer security techniques in wireless communication systems: a review”European Journal of Engineering and Technology Vol. 5 No. 1, 2017.

[11] S. Goel and R. Negi, “Guaranteeing secrecy using artificialnoise,” IEEE Transactions on Wireless Communications, vol. 7,no. 6, pp. 2180–2189, 2008.

[12] Ahsan Aziz "Decision Feedback Equalizer for StarCore®-Based DSPs" Freescale Semiconductor, 2007.

[13] Heyi Sun, AnantSahai, Ed, John Wawrzynek, Ed.“Spectrum Access System: Design and Implementation of the Decision-Feedback Equalizer in Software”http://www2.eecs.berkeley.edu/Pubs/TechRpts /2017/EECS-2017-83.pdf may 2017

[14] M. Moshfegh, Al. Rahmati and A.Hajisami “Optimized Decision Feedback Equalizer and Comparison with MLSE Algorithm for GSM Channel” IEEEInternational Conference on Modelling and Simulation, May 2011.

[15] P. Lioliou, M. Viberg, M. Coldrey, and F. Athley, “Self-interferencesuppression in full-duplex MIMO relays,” in 2010 Conference Recordof the Forty Fourth Asilomar Conference on Signals, Systems andComputers, Nov 2010, pp. 658–662.